EFFICIENT AND ROBUST VIDEO STEGANOGRAPHY ALGORITHMS FOR SECURE DATA COMMUNICATION

Ramadhan J. Mstafa and Khaled M. Elleithy

Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT 06604, USA

rmstafa@my.bridgeport.edu, *elleithy@bridgeport.edu*

ABSTRACT

Nowadays, the science of information hiding has gained tremendous significance due to advances in information and communication technology. The performance of any steganography method relies on the imperceptibility, embedding capacity, and robustness against attacks. This research provides solutions for the existing video steganography problems by proposing new and effective methods for digital video steganography. The key objectives of our paper are as follows: 1) a highly secure video steganography algorithm based on error correcting codes (ECC); 2) an increased payload video steganography algorithm in the discrete wavelet domain based on ECC; 3) a novel video steganography algorithm based on Kanade-Lucas-Tomasi (KLT) tracking and ECC; 4) a robust video steganography algorithm in the wavelet domain based on KLT tracking and ECC; and 5) a video steganography algorithm based on multiple object tracking and ECC. The experimental results from our research demonstrate that our proposed algorithms achieve higher embedding capacity as well as better imperceptibility of stego videos. Furthermore, the preprocessing stages increase the security and robustness of the proposed algorithms against attacks when compared to state-of-the-art steganographic methods.

Index Terms— Video steganography, imperceptibility, embedding capacity, robustness, KLT, and ECC.

1. INTRODUCTION

In spite of the fact that the Internet is utilized as a well-known provider for users to access desired information, it has also opened a new door for attackers to obtain precious information of other users with little effort [1]. Steganography is characterized as the art of concealing secret information in specific carrier data, establishing covert communication channels between official parties [2]. Subsequently, a stego object should be same as an original data that has the same statistical features. Embedding efficiency, embedding capacity, and robustness are the three major requirements incorporated in any successful steganographic methods [3]. First, the steganography method is highly efficient if it includes encryption, imperceptibility, and undetectability characteristics. The high efficient algorithm embeds the secret message into the carrier data by utilizing some of the encoding and encryption techniques prior to the embedding process to enhance the security of the algorithm [4]. The embedding capacity is the second fundamental requirement which permits any steganography method to extend the size of hidden message taking into account the visual quality of steganograms. Robustness is the third requirement which calculates the steganographic method's strength against attacks and signal processing [5].

2. MOTIVATIONS AND RESEARCH PROBLEM

Due to the significant growth of video data over the Internet, video steganography has become an important topic in signal processing research areas. Recently, a large number of video steganography algorithms have been proposed in various literature. Unfortunately, many of these algorithms lack the preprocessing stages. Particularly, there is no video steganography algorithm that includes preprocessing stages for both secret messages and cover videos. Moreover, existing steganography techniques suffer major weakness in several aspects including security, embedding capacity, imperceptibility, and robustness against attacks.

Our research is motivated by the limitations of existing video steganography algorithms, and based on the following reasons to improve the performance of these algorithms:

- By utilizing the preprocessing stages to include the procedure of manipulating both secret messages and cover videos prior to the embedding stage in order to enhance the security and robustness of the steganographic method.

- Using a portion of each video frame as regions of interest for the embedding process, the imperceptibility of stego videos will improve. Accordingly, we track the facial regions and moving objects in video. Since it is very challenging for attackers to determine the location of the secret message in video frames because the secret message is only embedded into facial regions and moving objects which changes from frame to frame, it is necessary to preserve the security and robustness of embedded data.

- Applying encryption methods and ECC such as Hamming codes and BCH codes to encode the secret massage prior to the embedding process will produce a secure and robust steganographic algorithm.

- Transforming video frames into frequency domain such as DWT and DCT transformations will improve the robustness of the steganographic method against attacks, hence preserving imperceptibility of stego videos.

3. METHODOLOGICAL APPROACHES

Our research investigates some innovative approaches to improve video steganography methods. The main objective of this paper is to develop and validate a new method to outperform the existing video steganography techniques from the literature [6]. In this research, the key contributions are as follows:

1. A highly secure video steganography algorithm based on ECC is proposed [7, 8]. In order to enhance the security and robustness of this algorithm against attacks, the secret message is embedded into specific areas of each video frame, randomly. The algorithm achieves better imperceptibility of stego videos as well as higher embedding capacity of secret data.

2. Increased payload video steganography algorithms in wavelet and cosine transformations based on ECC is proposed [9-11]. This method not only improved the capacity of the encoded secret message, but also increased the robustness against attackers, providing a reasonable tradeoff with the imperceptibility.

3. A novel video steganography algorithm based on KLT tracking and ECC is proposed, which controls the limitations of some state-of-the-art steganographic algorithms in terms of security

and imperceptibility [12]. This algorithm utilizes facial regions as carrier data to conceal the secret message, which operates in spatial. **Fig. 1** illustrates the framework of our third proposed algorithm.

4. A robust video steganography algorithm in the wavelet domain based on KLT tracking and ECC is proposed [13]. This method uses wavelet coefficients of facial regions as cover data to embed the secret information, hence enhancing the security and robustness of the hidden data.

5. A video steganography algorithm based on multiple object tracking and ECC is proposed [14]. Such algorithm will use multiple moving objects in video as cover data to embed the secret message, such as concealing the secret message into the region of interest including the human body, cars, or any other motion objects inside the digital video. **Fig. 2** shows the framework of our fifth algorithm.

4. CONCLUSION

The main objective of this research is to enhance video steganography methods. Hence, new algorithms are developed to maintain a reasonable trade-off between imperceptibility, hiding capacity, and robustness against various attacks. Our experimental results demonstrate that the proposed algorithms achieve higher embedding capacity as well as better visual quality of stego videos. Furthermore, the preprocessing steps increase the security and robustness of the proposed algorithms when compared to state-of-the-art methods.

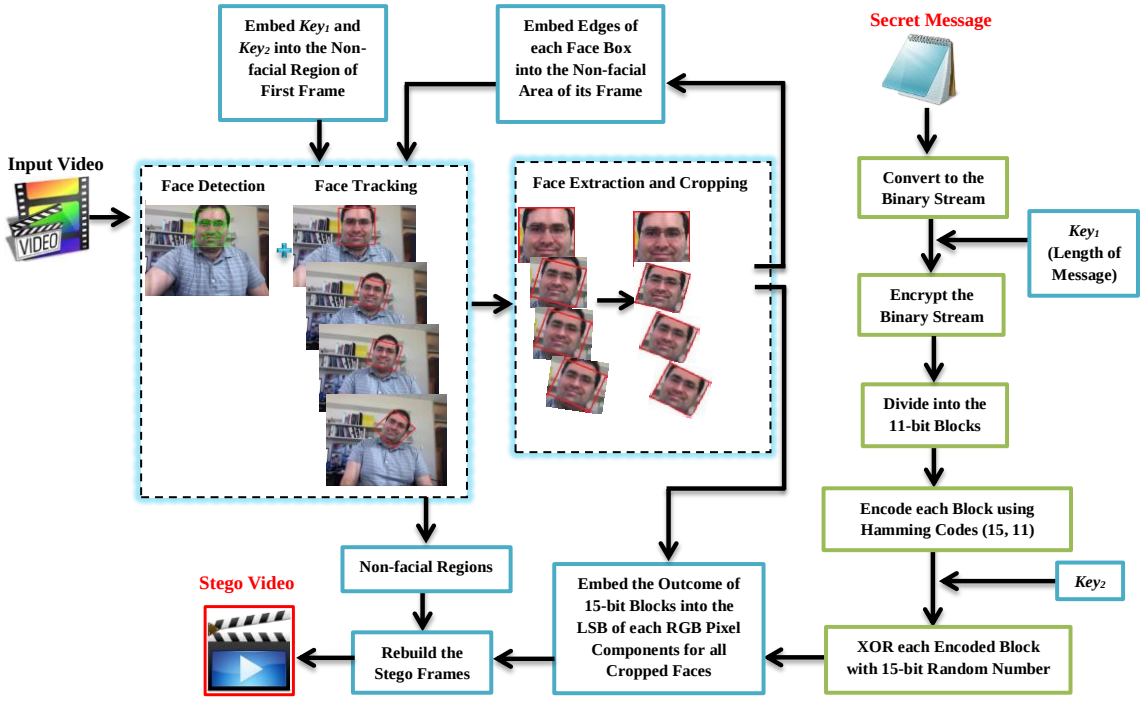

Fig. 1. Framework of our third proposed algorithm [12].

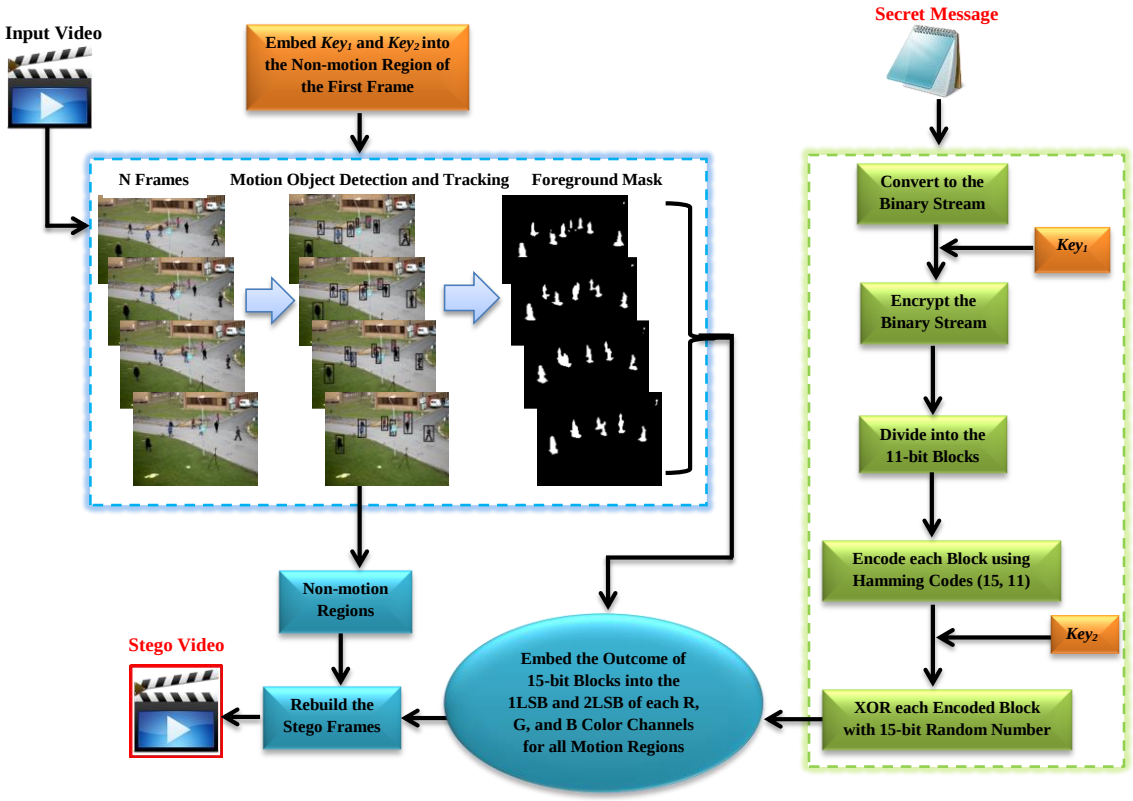

Fig. 2. Framework of data embedding stage for our fifth algorithm [14].

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "A secure and improved self-embedding algorithm to combat digital document forgery," *Signal Processing*, vol. 89, pp. 2324-2332, 2009.

[2] X.-y. Wang, C.-p. Wang, H.-y. Yang, and P.-p. Niu, "A robust blind color image watermarking in quaternion Fourier transform domain," *Journal of Systems and Software*, vol. 86, pp. 255-277, 2013.

[3] M. Hasnaoui and M. Mitrea, "Multi-symbol QIM video watermarking," *Signal Processing: Image Communication*, vol. 29, pp. 107-127, 2014.

[4] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "Adaptive Steganography Based on Syndrome-Trellis Codes and Local Complexity," in *2012 Fourth International Conference on Multimedia Information Networking and Security (MINES)*, 2012, pp. 323-327.

[5] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," *Information Sciences*, vol. 279, pp. 251-272, 2014.

[6] R. J. Mstafa and K. M. Elleithy, "Compressed and raw video steganography techniques: a comprehensive survey and analysis," *Multimedia Tools and Applications*, pp. 1-38, 2016.

[7] R. J. Mstafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," in *2014 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2014, pp. 1-6.

[8] R. J. Mstafa and K. M. Elleithy, "An Efficient Video Steganography Algorithm Based on BCH Codes," in *American Society for Engineering Education (ASEE Zone 1) Conference*, 2015, pp. 1-10.

[9] R. J. Mstafa and K. M. Elleithy, "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)," in *Wireless Telecommunications Symposium (WTS)*, 2015, pp. 1-8.

[10] R. J. Mstafa and K. M. Elleithy, "A DCT-based robust video steganographic method using BCH error correcting codes," in *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2016, pp. 1-6.

[11] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in DCT domain based on hamming and BCH codes," in *2016 IEEE 37th Sarnoff Symposium*, 2016, pp. 208-213.

[12] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimedia Tools and Applications*, vol. 75, pp. 10311-10333, 2016.

[13] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," in *2015 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2015, pp. 1-7.

[14] R. J. Mstafa and K. M. Elleithy, "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes," in *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, 2015, pp. 335-340.